Software Assurance: Highlighting Changes Within Our Software Community of Practice

In an era riddled with asymmetric cyber attacks, claims about system reliability, integrity and safety must also include provisions for built-in security of the enabling software. To facilitate changes and adoption of requisite practices, the Departments of Homeland Security (DHS) and Defense (DoD) are investing in *Software Assurance* by partnering with software practitioners in industry, government, and academia to increase the availability and use of tools, knowledge, and guidance that will help improve the security and quality of the software used in national security systems and critical infrastructure.

How is Software Assurance influencing our software community of practice and addressing relevant needs? Over time, we learn to do what needs to change, and we share practices. From the users' perspective, we have learned that development and acquisition practices should only be categorized as *best practices* if they contribute to the delivery of safe and secure products, systems and services. Developers have continued questioning their assumptions about how software should be built. They have a growing understanding that functional correctness must be exhibited not only when the software executes under anticipated conditions but also when it is subjected to unanticipated, hostile conditions. Acquirers have a better understanding that more scrutiny is needed of their supply chains to reduce the risk exposures being passed to users of software and software-intensive systems. Interaction among practitioners continually refines and develops the elements of practice. This is why relevant knowledge and skills have limited shelf-lives that prompt competency *refresh* requirements.

An organization's software community of practice is critical to its success. The community may exist informally within and across business units and projects and often across organizational boundaries. To gain the most leverage, it maintains links outside the organization to strengthen its knowledge base. Communities of practice are organizational assets because of the knowledge they steward at their core and through the learning they inspire at their boundaries. The learning potential of an organization resides in the interaction of cores and boundaries in *constellations* or clusters of different communities of practices. Indeed, software assurance is derived from the application of integrated processes and practices from multiple disciplines, requiring software practitioners to interact with other communities of practice (such as systems engineering, program management, security, etc.).

Our software community of practice develops resources such as shared learning and practices. Several organizations facilitate the capture and transfer of knowledge critical to our software community practitioners. CrossTalk functions as one of our software community's key conduits for transferring knowledge, and the DHS BuildSecurityIn Web site is evolving as an online resource at <http://BuildSecurityIn.us-cert.gov>.

The DHS Software Assurance Program provides a framework to shape a comprehensive strategy that addresses people, process, technology and acquisition throughout the software life cycle. Our efforts seek to shift the paradigm away from patch management and to achieve a broader ability to routinely develop and deploy trustworthy software products; contributing to the production of higher quality, more secure software. Through hosting and co-hosting various forums, we have leveraged collaborative efforts of public-private working groups. DHS initiatives, such as a software assurance common body of knowledge, guides for developers and acquisition managers, and the *BuildSecurityIn* Web site will continue to evolve and provide practical guidance on how to improve the quality, reliability, and security of software.

This DHS-sponsored issue of CrossTalk addresses not only the value of software assurance, but also various methods in achieving it. I hope readers will take the time to understand and apply the principles and techniques. I encourage everyone to discover more about our Software Assurance efforts and learn more about proven security practices by reviewing our DHS BuildSecurityIn Web site and joining others in our expanding software assurance community of practice.

Joe Jarzombek

Joe Jarzombek, Project Management Professional (USAF Lt. Col., Retired)
Director for Software Assurance
National Cyber Security Division
Department of Homeland Security